(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－66706

(43)公開日　平成11年(1999)３月９日

(51)Int.Cl.⁶		識別記号	FI		
Ｇ１１Ｂ	19/04	５０１	Ｇ１１Ｂ	19/04	５０１Ｈ
	7/00			7/00	Ｑ
	20/10			20/10	Ｄ
					Ｆ
	20/14	３４１		20/14	３４１Ａ

審査請求　未請求　請求項の数20　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平9－228234

(22)出願日　平成９年(1997)８月25日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　志村　成生
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

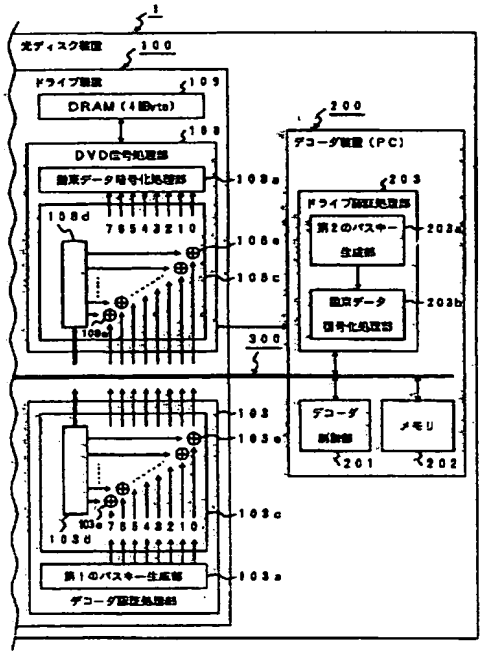
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　光ディスク再生装置及び光ディスク記録再生装置

(57)【要約】

【課題】光ディスクデータの不正コピーを防止することが可能な光ディスク再生装置及び光ディスク記録再生装置を提供すること。

【解決手段】光ディスクから光ディスクデータを読出し提供するドライブ装置（１００）と、光ディスクデータを再生するデコーダ装置（２００）と、各装置間及び各装置内のデータ通信を担う通信手段（３００）とを備えた光ディスク装置（１）において、光ディスクデータを暗号化する第１のデータを生成し提供するデータ生成手段（１０３ａ）と、第１のデータを暗号化して第２のデータを生成し、この第２のデータを前記通信手段を介して送信する暗号化手段（１０３ｃ）と、通信手段を介して第２のデータを受信し、この第２のデータを復号化して第１のデータを生成する復号化手段（１０８ｃ）とを備えている。



【特許請求の範囲】

【請求項１】光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、

前記光ディスクデータを暗号化するための暗号化用データを生成し提供する暗号化用データ生成手段と、

前記通信手段と所定の状態で接続されたものであって、前記暗号化用データを前記通信手段へ出力する出力手段と、

前記通信手段と前記所定の状態と同一の状態で接続されたものであって、前記通信手段を介して前記暗号化用データを入力する入力手段と、

を備えたことを特徴とする光ディスク再生装置。

【請求項２】光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、

前記ドライブ装置側に設けられたものであって、前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、

前記ドライブ装置側に設けられ、且つ前記通信手段と所定の状態で接続されたものであって、前記第１の暗号化用データを前記通信手段へ出力する出力手段と、

前記ドライブ装置側に設けられ、且つ前記通信手段と前記所定の状態と同一の状態で接続されたものであって、前記通信手段を介して前記第１の暗号化用データを入力する入力手段と、

前記ドライブ装置側に設けられたものであって、前記入力手段から入力された前記第１の暗号化用データにより第１の光ディスクデータに対して暗号化処理を施し、この第１の光ディスクデータから第２の光ディスクデータを生成し、この第２の光ディスクデータを前記通信手段を介して前記デコーダ装置側へ提供する暗号化処理手段と、

前記デコーダ装置側に設けられたものであって、前記光ディスクデータを暗号化するための前記第１の暗号化用データと同一の第２の暗号化用データを生成し提供する第２の暗号化用データ生成手段と、

前記デコーダ装置側に設けられたものであって、前記通信手段を介して前記第２の光ディスクデータを受取り、前記第２の暗号化用データによりこの第２の光ディスクデータに対して復号化処理を施し、この第２の光ディスクデータから前記第１の光ディスクデータを生成し提供する復号化処理手段と、

を備えたことを特徴とする光ディスク再生装置。

【請求項３】光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、

前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、

前記第１の暗号化用データに対して暗号化処理を施し、この第１の暗号化用データから第２の暗号化用データを生成し、この第２の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、

前記通信手段を介して前記第２の暗号化用データを受信し、この第２の暗号化用データに対して復号化処理を施し、この第２の暗号化用データから前記第１の暗号化用データを生成し提供する復号化処理手段と、

を備えたことを特徴とする光ディスク再生装置。

【請求項４】光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、

前記ドライブ装置側に設けられたものであって、前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、

前記ドライブ装置側に設けられたものであって、前記第１の暗号化用データに対して暗号化処理を施し、この第１の暗号化用データから第２の暗号化用データを生成し、この第２の暗号化用データを前記通信手段を介して送信する第１の暗号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記通信手段を介して前記第２の暗号化用データを受信し、この第２の暗号化用データに対して復号化処理を施し、この第２の暗号化用データから前記第１の暗号化用データを生成し提供する第１の復号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記第１の復号化処理手段により生成された前記第１の暗号化用データにより第１の光ディスクデータに対して暗号化処理を施し、この第１の光ディスクデータから第２の光ディスクデータを生成し、この第２の光ディスクデータ

を前記通信手段を介して前記デコーダ装置側へ提供する第２の暗号化処理手段と、
前記デコーダ装置側に設けられたものであって、前記光ディスクデータを暗号化するための前記第１の暗号化用データと同一の第３の暗号化用データを生成し提供する第３の暗号化用データ生成手段と、
前記デコーダ装置側に設けられたものであって、前記通信手段を介して前記第２の光ディスクデータを受取り、前記第３の暗号化用データによりこの第２の光ディスクデータに対して復号化処理を施し、この第２の光ディスクデータから前記第１の光ディスクデータを生成し提供する第２の復号化処理手段と、
を備えたことを特徴とする光ディスク再生装置。
【請求項５】光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、
前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、
前記第１の暗号化用データを暗号化するための第２の暗号化用データを生成し提供する第２の暗号化用データ生成手段と、
前記第２の暗号化データにより前記第１の暗号化用データに対して暗号化処理を施し、前記第１の暗号化用データから第３の暗号化用データを生成し、この第３の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、
前記通信手段を介して前記第２及び第３の暗号化用データを受信し、この第２の暗号化用データによりこの第３の暗号化用データに対して復号化処理を施し、この第３の暗号化用データから第１の暗号化用データを生成し提供する復号化処理手段と、
を備えたことを特徴とする光ディスク再生装置。
【請求項６】前記暗号化処理手段が、前記第１の暗号化用データと前記第２の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第３の暗号化用データとして提供する第１の排他的論理和算出手段を有し、
前記復号化処理手段が、前記第２の暗号化用データと前記第３の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第１の暗号化用データとして提供する第２の排他的論理和算出手段を有する、
ことを特徴とする請求項５に記載の光ディスク再生装置。
【請求項７】光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、
前記ドライブ装置側に設けられたものであって、前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、
前記ドライブ装置側に設けられたものであって、前記第１の暗号化用データを暗号化するための第２の暗号化用データを生成し提供する第２の暗号化用データ生成手段と、
前記ドライブ装置側に設けられたものであって、前記第２の暗号化データにより前記第１の暗号化用データに対して暗号化処理を施し、前記第１の暗号化用データから第３の暗号化用データを生成し、この第３の暗号化用データを前記通信手段を介して送信する第１の暗号化処理手段と、
前記ドライブ装置側に設けられたものであって、前記通信手段を介して前記第２及び第３の暗号化用データを受信し、この第２の暗号化用データによりこの第３の暗号化用データに対して復号化処理を施し、この第３の暗号化用データから第１の暗号化用データを生成し提供する第１の復号化処理手段と、
前記ドライブ装置側に設けられたものであって、前記第１の復号化処理手段により生成された前記第１の暗号化用データにより第１の光ディスクデータに対して暗号化処理を施し、この第１の光ディスクデータから第２の光ディスクデータを生成し、この第２の光ディスクデータを前記通信手段を介して前記デコーダ装置側へ提供する第２の暗号化処理手段と、
前記デコーダ装置側に設けられたものであって、前記光ディスクデータを暗号化するための前記第１の暗号化用データと同一の第４の暗号化用データを生成し提供する第４の暗号化用データ生成手段と、
前記デコーダ装置側に設けられたものであって、前記通信手段を介して前記第２の光ディスクデータを受取り、前記第４の暗号化用データによりこの第２の光ディスクデータに対して復号化処理を施し、この第２の光ディスクデータから前記第１の光ディスクデータを生成し提供する第２の復号化処理手段と、
を備えたことを特徴とする光ディスク再生装置。
【請求項８】前記第１の暗号化処理手段が、前記第１の暗号化用データと前記第２の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第３の暗号化用データとして提供する第１の排他的論理和算出手段を有し、
前記第１の復号化処理手段が、前記第２の暗号化用デー

タと前記第３の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第１の暗号化用データとして提供する第２の排他的論理和算出手段を有する、ことを特徴とする請求項７に記載の光ディスク再生装置。

【請求項９】前記第２の暗号化用データ生成手段が時間とともに変化する乱数を生成し、この乱数を前記第２の暗号化用データとして提供する乱数生成手段を有することを特徴とする請求項５又は請求項７に記載の光ディスク再生装置。

【請求項１０】前記第２の暗号化用データ生成手段における前記第２の暗号化用データの生成を制御する制御プログラムを記憶する記憶手段と、

前記制御プログラムに基づき前記第２の暗号化用データ生成手段における前記第２の暗号化用データの生成を制御する制御手段と、

を有することを特徴とする請求項５又は請求項７に記載の光ディスク再生装置。

【請求項１１】光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、

前記光ディスクデータを暗号化するための暗号化用データを生成し提供する暗号化用データ生成手段と、

前記通信手段と所定の状態で接続されたものであって、前記暗号化用データを前記通信手段へ出力する出力手段と、

前記通信手段と前記所定の状態と同一の状態で接続されたものであって、前記通信手段を介して前記暗号化用データを入力する入力手段と、

を備えたことを特徴とする光ディスク記録再生装置。

【請求項１２】光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、

前記ドライブ装置側に設けられたものであって、前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、

前記ドライブ装置側に設けられ、且つ前記通信手段と所定の状態で接続されたものであって、前記第１の暗号化用データを前記通信手段へ出力する出力手段と、

前記ドライブ装置側に設けられ、且つ前記通信手段と前記所定の状態と同一の状態で接続されたものであって、前記通信手段を介して前記第１の暗号化用データを入力する入力手段と、

前記ドライブ装置側に設けられたものであって、前記入力手段から入力された前記第１の暗号化用データにより第１の光ディスクデータに対して暗号化処理を施し、この第１の光ディスクデータから第２の光ディスクデータを生成し、この第２の光ディスクデータを前記通信手段を介して前記デコーダ装置側へ提供する暗号化処理手段と、

前記デコーダ装置側に設けられたものであって、前記光ディスクデータを暗号化するための前記第１の暗号化用データと同一の第２の暗号化用データを生成し提供する第２の暗号化用データ生成手段と、

前記デコーダ装置側に設けられたものであって、前記通信手段を介して前記第２の光ディスクデータを受取り、前記第２の暗号化用データによりこの第２の光ディスクデータに対して復号化処理を施し、この第２の光ディスクデータから前記第１の光ディスクデータを生成し提供する復号化処理手段と、

を備えたことを特徴とする光ディスク記録再生装置。

【請求項１３】光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、

前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、

前記第１の暗号化用データに対して暗号化処理を施し、この第１の暗号化用データから第２の暗号化用データを生成し、この第２の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、

前記通信手段を介して前記第２の暗号化用データを受信し、この第２の暗号化用データに対して復号化処理を施し、この第２の暗号化用データから前記第１の暗号化用データを生成し提供する復号化処理手段と、

を備えたことを特徴とする光ディスク記録再生装置。

【請求項１４】光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクから

の反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、

前記ドライブ装置側に設けられたものであって、前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、

前記ドライブ装置側に設けられたものであって、前記第１の暗号化用データに対して暗号化処理を施し、この第１の暗号化用データから第２の暗号化用データを生成し、この第２の暗号化用データを前記通信手段を介して送信する第１の暗号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記通信手段を介して前記第２の暗号化用データを受信し、この第２の暗号化用データに対して復号化処理を施し、この第２の暗号化用データから前記第１の暗号化用データを生成し提供する第１の復号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記第１の復号化処理手段により生成された前記第１の暗号化用データにより第１の光ディスクデータに対して暗号化処理を施し、この第１の光ディスクデータから第２の光ディスクデータを生成し、この第２の光ディスクデータを前記通信手段を介して前記デコーダ装置側へ提供する第２の暗号化処理手段と、

前記デコーダ装置側に設けられたものであって、前記光ディスクデータを暗号化するための前記第１の暗号化用データと同一の第３の暗号化用データを生成し提供する第３の暗号化用データ生成手段と、

前記デコーダ装置側に設けられたものであって、前記通信手段を介して前記第２の光ディスクデータを受取り、前記第３の暗号化用データによりこの第２の光ディスクデータに対して復号化処理を施し、この第２の光ディスクデータから前記第１の光ディスクデータを生成し提供する第２の復号化処理手段と、

を備えたことを特徴とする光ディスク記録再生装置。

【請求項１５】光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、

前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、

前記第１の暗号化用データを暗号化するための第２の暗号化用データを生成し提供する第２の暗号化用データ生成手段と、

前記第２の暗号化データにより前記第１の暗号化用データに対して暗号化処理を施し、前記第１の暗号化用データから第３の暗号化用データを生成し、この第３の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、

前記通信手段を介して前記第２及び第３の暗号化用データを受信し、この第２の暗号化用データによりこの第３の暗号化用データに対して復号化処理を施し、この第３の暗号化用データから第１の暗号化用データを生成し提供する復号化処理手段と、

を備えたことを特徴とする光ディスク記録再生装置。

【請求項１６】前記暗号化処理手段が、前記第１の暗号化用データと前記第２の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第３の暗号化用データとして提供する第１の排他的論理和算出手段を有し、

前記復号化処理手段が、前記第２の暗号化用データと前記第３の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第１の暗号化用データとして提供する第２の排他的論理和算出手段を有する、

ことを特徴とする請求項１５に記載の光ディスク記録再生装置。

【請求項１７】光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、

前記ドライブ装置側に設けられたものであって、前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、

前記ドライブ装置側に設けられたものであって、前記第１の暗号化用データを暗号化するための第２の暗号化用データを生成し提供する第２の暗号化用データ生成手段と、

前記ドライブ装置側に設けられたものであって、前記第２の暗号化データにより前記第１の暗号化用データに対して暗号化処理を施し、前記第１の暗号化用データから第３の暗号化用データを生成し、この第３の暗号化用データを前記通信手段を介して送信する第１の暗号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記通

信手段を介して前記第２及び第３の暗号化用データを受信し、この第２の暗号化用データによりこの第３の暗号化用データに対して復号化処理を施し、この第３の暗号化用データから第１の暗号化用データを生成し提供する第１の復号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記第１の復号化処理手段により生成された前記第１の暗号化用データにより第１の光ディスクデータに対して暗号化処理を施し、この第１の光ディスクデータから第２の光ディスクデータを生成し、この第２の光ディスクデータを前記通信手段を介して前記デコーダ装置側へ提供する第２の暗号化処理手段と、

前記デコーダ装置側に設けられたものであって、前記光ディスクデータを暗号化するための前記第１の暗号化用データと同一の第４の暗号化用データを生成し提供する第４の暗号化用データ生成手段と、

前記デコーダ装置側に設けられたものであって、前記通信手段を介して前記第２の光ディスクデータを受取り、前記第４の暗号化用データによりこの第２の光ディスクデータに対して復号化処理を施し、この第２の光ディスクデータから前記第１の光ディスクデータを生成し提供する第２の復号化処理手段と、

を備えたことを特徴とする光ディスク記録再生装置。

【請求項１８】前記第１の暗号化処理手段が、前記第１の暗号化用データと前記第２の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第３の暗号化用データとして提供する第１の排他的論理和算出手段を有し、

前記第１の復号化処理手段が、前記第２の暗号化用データと前記第３の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第１の暗号化用データとして提供する第２の排他的論理和算出手段を有する、ことを特徴とする請求項１７に記載の光ディスク記録再生装置。

【請求項１９】前記第２の暗号化用データ生成手段が時間とともに変化する乱数を生成し、この乱数を前記第２の暗号化用データとして提供する乱数生成手段を有することを特徴とする請求項１５又は請求項１７に記載の光ディスク記録再生装置。

【請求項２０】前記第２の暗号化用データ生成手段における前記第２の暗号化用データの生成を制御する制御プログラムを記憶する記憶手段と、

前記制御プログラムに基づき前記第２の暗号化用データ生成手段における前記第２の暗号化用データの生成を制御する制御手段と、

を有することを特徴とする請求項１５又は請求項１７に記載の光ディスク記録再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、光ディスクに記録されている光ディスクデータを再生する光ディスク再生装置、及び光ディスクに記録されている光ディスクデータの再生並びに光ディスクに対するデータの記録を行う光ディスク記録再生装置に関する。特に、光ディスクデータの不正コピーを防止するため、必要に応じて光ディスクデータを暗号化する光ディスク再生装置、及び光ディスク記録再生装置に関する。

【０００２】

【従来の技術】近年、大容量情報記憶媒体としてＤＶＤ（Digital Video Disk）－ＲＯＭ及びＤＶＤ－ＲＡＭ等の光ディスクが注目をあびている。前者は再生専用の情報記憶媒体であり、後者は書換え可能な情報記録媒体である。

【０００３】ここで、このような光ディスクに記録されている光ディスクデータを再生する光ディスク再生装置、及びこのような光ディスクに記録されている光ディスクデータの再生並びに光ディスクに対するデータの記録を行う光ディスク記録再生装置について簡単に説明する。なお、ここでは、光ディスク再生装置及び光ディスク記録再生装置の両者を併せて光ディスク装置と称する。

【０００４】光ディスク装置は、例えば、ドライブ装置、デコータ装置（パーソナルコンピュータなど）、及びバスライン等より構成されている。ドライブ装置は、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するものである。デコーダ装置は、ドライブ装置から提供される光ディスクデータを再生するものである。バスラインは、ドライブ装置及びデコーダ装置の間のデータ通信、並びにドライブ装置内及びデコーダ装置内のデータ通信を担うものである。

【０００５】また、ドライブ装置には、第１のバスキー生成部及び暗号化処理部が設けられている。第１のバスキー生成部ではバスキーなるものが生成される。この第１のバスキー生成部で生成されたバスキーは、バスラインを介して暗号化処理部へ送信される。暗号化処理部では、送信されたバスキーにより光ディスクデータに対して暗号化処理が施される。

【０００６】デコーダ装置には、第２のバスキー生成部及び復号化処理部が設けられている。第２のバスキー生成部では、第１のバスキー生成部で生成されるバスキーと同一のバスキーが生成される。この第２のバスキー生成部で生成されたバスキーは、復号化処理部へ送信される。復号化処理部では、送信されたバスキーにより暗号化された光ディスクデータに対して復号化処理が施される。

【０００７】ドライブ装置側からデコーダ装置側へバスラインを介して光ディスクデータを送信する場合、光ディスクデータはドライブ装置側（第１のバスキー生成部）で生成されたバスキーにより暗号化されてから送信

される。つまり、デコータ装置側では、暗号化された光ディスクデータが受信される。そして、デコーダ装置側では、このデコーダ装置側（第２のバスキー生成部）で生成されたバスキーにより暗号化された光ディスクデータが復号化される。

【０００８】このように、バスラインを介して送信される光ディスクデータを暗号化することにより、バスライン上における光ディスクデータのセキュリティが確保されている。具体的に説明すると、光ディスクデータを不正にコピーしようとする者が、バスラインから光ディスクデータを読出したとしても、読出された光ディスクデータは暗号化されているため、この者の目的は達成されないというものである。

【０００９】

【発明が解決しようとする課題】ところが、このような光ディスク装置の場合、バスライン上のデータが解析されることにより、バスキーが解読されてしまい、その結果、光ディスクデータが不正にコピーされてしまうという問題点があった。

【００１０】つまり、バスキーが解読されてしまうと、バスキーにより暗号化された光ディスクデータは、暗号化されていないもの同然となってしまう。よって、光ディスクデータが不正にコピーされてしまうということになる。

【００１１】この発明の目的は、上記したような事情に鑑み成されたものであって、光ディスクデータの不正コピーを防止することが可能な光ディスク再生装置及び光ディスク記録再生装置を提供することにある。

【００１２】

【課題を解決するための手段】上記課題を解決し目的を達成するために、この発明の光ディスク再生装置及び光ディスク記録再生装置は、以下のように構成されている。

（１）この発明は、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、前記光ディスクデータを暗号化するための暗号化用データを生成し提供する暗号化用データ生成手段と、前記通信手段と所定の状態で接続されたものであって、前記暗号化用データを前記通信手段へ出力する出力手段と、前記通信手段と前記所定の状態と同一の状態で接続されたものであって、前記通信手段を介して前記暗号化用データを入力する入力手段とを備えている。

【００１３】（２）この発明は、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、前記第１の暗号化用データに対して暗号化処理を施し、この第１の暗号化用データから第２の暗号化用データを生成し、この第２の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、前記通信手段を介して前記第２の暗号化用データを受信し、この第２の暗号化用データに対して復号化処理を施し、この第２の暗号化用データから前記第１の暗号化用データを生成し提供する復号化処理手段とを備えている。

【００１４】（３）この発明は、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、前記第１の暗号化用データを暗号化するための第２の暗号化用データを生成し提供する第２の暗号化用データ生成手段と、前記第２の暗号化データにより前記第１の暗号化用データに対して暗号化処理を施し、前記第１の暗号化用データから第３の暗号化用データを生成し、この第３の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、前記通信手段を介して前記第２及び第３の暗号化用データを受信し、この第２の暗号化用データによりこの第３の暗号化用データに対して復号化処理を施し、この第３の暗号化用データから第１の暗号化用データを生成し提供する復号化処理手段とを備えている。

【００１５】（４）この発明は、光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、前記光ディスクデータを暗号化するための暗号化用データを生成し提供する暗号化用データ生成手段と、前記通信手段と所定の状態で接続されたものであって、前記暗号化用データを前記通信

手段へ出力する出力手段と、前記通信手段と前記所定の状態と同一の状態で接続されたものであって、前記通信手段を介して前記暗号化用データを入力する入力手段とを備えている。

【００１６】（５）この発明は、光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、前記第１の暗号化用データに対して暗号化処理を施し、この第１の暗号化用データから第２の暗号化用データを生成し、この第２の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、前記通信手段を介して前記第２の暗号化用データを受信し、この第２の暗号化用データに対して復号化処理を施し、この第２の暗号化用データから前記第１の暗号化用データを生成し提供する復号化処理手段とを備えている。

【００１７】（６）この発明は、光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、前記光ディスクデータを暗号化するための第１の暗号化用データを生成し提供する第１の暗号化用データ生成手段と、前記第１の暗号化用データを暗号化するための第２の暗号化用データを生成し提供する第２の暗号化用データ生成手段と、前記第２の暗号化データにより前記第１の暗号化用データに対して暗号化処理を施し、前記第１の暗号化用データから第３の暗号化用データを生成し、この第３の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、前記通信手段を介して前記第２及び第３の暗号化用データを受信し、この第２の暗号化用データによりこの第３の暗号化用データに対して復号化処理を施し、この第３の暗号化用データから第１の暗号化用データを生成し提供する復号化処理手段とを備えている。

【００１８】上記手段を講じた結果、光ディスクデータを暗号化するためのデータが、暗号化された上で通信手段を介して送信される。これにより、光ディスクデータを暗号化するためのデータの解析を困難なものとすることが可能となる。

【００１９】

【発明の実施の形態】以下、この発明の実施の形態について図面を参照して説明する。図１は、この発明の一実施の形態に係る光ディスク装置（光ディスク再生装置及び光ディスク記録再生装置）の概略構成を示す図である。

【００２０】図１に示すように、光ディスク装置１は、ドライブ装置１００、デコーダ装置２００、通信手段としてのバスライン３００等により構成されている。ドライブ装置１００には、ドライブ制御部１０１、メモリ１０２、デコーダ認証処理部１０３、レーザ駆動制御部１０４、光ピックアップ部１０５、アナログ信号処理部１０６、サーボ制御部１０７、ＤＶＤ信号処理部１０８、ＤＲＡＭ１０９、ＣＤ（Compact Disc）信号処理部１１０、ＤＲＡＭ１１１等が設けられている。

【００２１】また、光ピックアップ部１０５には、半導体レーザ１０５ａ、及び光検出器１０５ｂ等が設けられている。さらに、光ディスク装置１が光ディスク記録再生装置の場合には、ドライブ装置１００には、記録用データ処理部１１２が設けられている。なお、上記したドライブ制御部１０１、メモリ１０２、デコーダ認証処理部１０３、ＤＶＤ信号処理部１０８、及び記録用データ処理部１１２は、バスライン３００に接続されている。

【００２２】ドライブ制御部１０１は、メモリ１０２に記憶されたドライブ制御プログラムに基づきドライブ装置１００全体を制御するものである。デコーダ認証処理部１０３は、後述する相互認証処理によりデコーダ装置を認証するものである。レーザ駆動制御部１０４は、半導体レーザ１０５ａを制御するものであり、この光ディスク装置が光ディスク再生装置の場合と光ビーム記録再生装置の場合とで機能が異なる。この光ディスク装置が光ディスク再生装置の場合には、レーザ駆動制御部１０４は、光ディスクに記録されたデータを再生するための再生用光ビームを半導体レーザ１０５ａから照射させる。この光ディスク装置が光ディスク記録再生装置の場合には、レーザ駆動制御部１０４は、光ディスクに記録されたデータを再生するための再生用光ビーム及び光ディスクにデータを記録するための記録用光ビームを照射させる。なお、レーザ駆動制御部１０４は、半導体レーザ１０５から記録用光ビームを照射させる際、記録用データ処理部１１４から提供される記録用データに基づき半導体レーザを制御する。

【００２３】光ピックアップ部１０５に設けられた光検出器１０５ｂは、半導体レーザ１０５ａから照射された再生用光ビームの光ディスクからの反射光を受光するものである。アナログ信号処理部１０６は、光検出器１０５ｂにより検出された光ディスクからの反射光を処理するものである。簡単に説明すると、反射光に反映された

光ディスクデータからＤＶＤ信号とＣＤ信号とを区別し、ＤＶＤ信号をサーボ制御部１０７及びＤＶＤ信号処理部１０８へ提供し、ＣＤ信号をＣＤ信号処理部１１０へ提供する。サーボ制御部１０７は、アナログ信号処理部１０６から提供されるＤＶＤ信号に基づき、フォーカス制御、トラッキング制御、及びリニアモータ制御を行うものである。ＤＶＤ信号処理部１０８は、アナログ信号処理部１０６から提供されるＤＶＤ信号に対して各種処理を施すものであり、このＤＶＤ信号処理部１０８については後に詳しく説明する。ＤＲＡＭ１０９は、例えば、４Ｍバイトの容量を有し、バッファとして機能する。ＣＤ信号処理部１１０は、アナログ信号処理部１０６から提供されるＣＤ信号に対して各種処理を施すものである。ＤＲＡＭ１１１は、例えば１２８Ｋバイトの容量を有し、バッファとして機能する。

【００２４】デコーダ装置２００には、デコーダ制御部２０１、メモリ２０２、及びドライブ認証処理部２０３等が設けられている。また、これら、デコーダ制御部２０１、メモリ２０２、及びドライブ認証処理部２０３は、バスライン３００に接続されている。

【００２５】デコーダ制御部２０１は、メモリ２０２に記憶されたデコーダ制御プログラムに基づきデコーダ装置２００全体を制御するものである。ドライブ認証処理部２０３は、後述する相互認証処理によりドライブ装置を認証するものである。

【００２６】続いて、ＤＶＤ－ＲＯＭ及びＤＶＤ－ＲＡＭのデータ構造について簡単に説明する。ＤＶＤ－ＲＯＭ及びＤＶＤ－ＲＡＭには、リードインエリア、データエリア、及びリードアウトエリアなどがフォーマットされている。これらエリアは、複数のゾーンで構成されており、各ゾーンは複数のトラックにより構成されている。また、リードインエリア内には、ＣＰＲ＿ＭＡＩ（Copyright Management Information）フィールド及びメインデータフィールドがフォーマットされている。同様に、データエリア内にも、ＣＰＲ＿ＭＡＩフィールド及びメインデータフィールドがフォーマットされている。

【００２７】リードインエリア内のＣＰＲ＿ＭＡＩ（Copyright Management Information）フィールドには、認証コード（Authentication Control code ）が記録されている。この認証コードは、ドライブ装置１００とデコーダ装置２００との相互認証の計算を行う際に用いられる５ビットのデータである。

【００２８】データアリア内のＣＰＲ＿ＭＡＩフィールドには、タイトルキー（EncryptedTitle Key ）が記録されている。このタイトルキーは、１枚の光ディスクの中に複数のタイトルが格納されている場合、これらタイトル夫々を暗号化する５バイトの鍵データである。

【００２９】リードインエリア内のメインデータフィールドには、ディスクキー（SecuredDisk Key Data ）が記録されている。このディスクキーは、１枚のディスクの中に複数のタイトルが格納されている場合、これらタイトルをディスク全体にわたって暗号化する２０４８バイトの共通の鍵データである。

【００３０】データエリア内のメインデータフィールドには、スクランブルＡＶデータが記録されている。このスクランブルＡＶデータは、図示しないスクランブラー（ブラックボックス）及びタイトルキーによりスクランブルされたＡＶデータである。

【００３１】続いて、ドライブ装置１００とデコーダ装置２００との間で行われる相互認証処理について説明する。ドライブ装置１００側には、既に説明したようにデコータ装置２００を認証するためのデコーダ認証部１０３が設けられている。同様に、デコーダ装置２００側にも、ドライブ装置１００を認証するためのドライブ認証部２０３が設けられている。相互認証処理は、ＣＰＲ＿ＭＡＩフィールドに記録されている認証コードを利用して進められる。ここで、認証コードを利用して進められる相互認証処理について具体的に説明する。

【００３２】はじめに、デコーダ装置２００のドライブ認証処理部２０３において、乱数を用いた８０ビットのチャレンジデータ１が生成される。このチャレンジデータ１は、デコーダ装置２００側からドライブ装置１００側へ送信され、ドライブ装置１００のデコーダ認証処理部１０３へ入力される。このデコーダ認証処理部１０３では、光ディスクから読出された認証コード及びチャレンジデータ１から４０ビットのレスポンスデータ１が計算される。このレスポンスデータ１は、ドライブ装置１００側からデコータ装置２００側へ送信され、デコータ装置２００のドライブ認証処理部２０３へ入力される。このドライブ認証処理部２０３では、チャレンジデータ１から計算された結果（４０ビットデータ）とレスポンスデータ１とを比較して、これらが等しいとき、ドライブ装置１００が認証される。

【００３３】次に、ドライブ装置１００のデコーダ認証処理部１０３において、乱数を用いた８０ビットのチャレンジデータ２が生成される。このチャレンジデータ２は、ドライブ装置１００側からデコーダ装置２００側へ送信され、デコーダ装置２００のドライブ認証処理部２０３へ入力される。このドライブ認証処理部２０３では、チャレンジデータ２から４０ビットのレスポンスデータ２が計算される。このレスポンスデータ２は、デコーダ装置２００側からドライブ装置１００側へ送信され、ドライブ装置１００のデコーダ認証処理部１０３へ入力される。このデコーダ認証処理部１０３では、チャレンジデータ２及び認証コードから計算された結果とレスポンスデータ２とを比較して、これらが等しいとき、デコーダ装置２００が認証される。

【００３４】デコーダ装置２００側でドライブ装置１００が認証され、ドライブ装置１００側でデコーダ装置２

００が認証されることにより、相互認証処理が完了する。続いて、デコーダ認証処理部１０３側で生成されたバスキーをバスライン３００を介してデコーダ認証処理部１０３側からＤＶＤ信号処理部１０８側へ送信し、このバスキーにより暗号化されたディスクキー及びタイトルキー（以下鍵束データと称する）をバスライン３００を介してドライブ装置１００側からデコーダ装置２００側へ送信する処理について説明する。

【００３５】まず、バスキーの送信処理その１について説明する。図２は、バスキーの送信処理その１を実現するための構成を示す図である。バスキーにより暗号化される鍵束データは、光ディスクから読取られ、ＤＶＤ信号処理回路１０８を経由して、ＤＲＡＭ１０９に書込まれる。

【００３６】図２に示すように、デコーダ認証処理部１０３には、暗号化用データ生成手段としての第１のバスキー生成部１０３ａ、及び出力手段としてのバスキー出力部１０３ｂが設けられている。第１のバスキー生成部１０３ａは、上記説明した相互認証処理によりドライブ装置及びデコーダ装置が相互に認証されることを条件として、第１のバスキーを生成するものである。この第１のバスキーは、鍵束データの暗号化に利用されるものである。バスキー出力部１０３ｂは、第１のバスキーをバスライン３００へ出力するものである。このバスキー出力部１０３ｂは、バスライン３００と図２に示すような特定の状態で接続するように構成されているものとする。つまり、このバスキー出力部１０３ｂから出力される第１のバスキーは、バスキー出力部１０３ｂがバスライン３００と特定の状態で接続されることにより、暗号化されてバスライン３００上へ出力されることになる。

【００３７】ＤＶＤ信号処理部１０８には、暗号化処理手段としての鍵束データ暗号化処理部１０８ａ、及び入力手段としてのバスキー入力部１０８ｂが設けられている。バスキー入力部１０８ｂは、バスキー出力部１０３ｂから出力された第１のバスキーをバスライン３００を介してＤＶＤ信号処理部１０８へ入力するものである。このバスキー入力部１０８ｂは、バスライン３００と図２に示すような特定の状態で接続するように構成されているものとする。つまり、バスキー出力部１０３ｂから出力された第１のバスキーが、このバスキー入力部１０８ｂを介して入力されることにより復号化されることになる。鍵束データ暗号化処理部１０８ａは、ＤＲＡＭ１０９から読出された鍵束データに対してバスキー入力部１０８ｂを介して得られた第１のバスキーにより暗号化処理を施し、暗号化処理済鍵束データを提供する。具体的に説明すると、鍵束データ暗号化処理部１０８ａは、鍵束データと第１のバスキーとの排他的論理和を算出する。つまり、ここで算出された排他的論理和の値が暗号化処理済鍵束データということになる。鍵束データ暗号化処理部１０８ａから提供される暗号化処理済鍵束データは、バスライン３００を介してデコーダ装置２００側へ送信される。

【００３８】ドライブ認証処理部２０３には、暗号化用データ生成手段としての第２のバスキー生成部２０３ａ、及び復号化処理手段としての鍵束データ復号化処理部２０３ｂが設けられている。第２のバスキー生成部２０３ａは、上記説明した相互認証処理によりドライブ装置及びデコーダ装置が相互に認証されことを条件として、第１のバスキーと同一のデータである第２のバスキーを生成する。この第２のバスキーは、第１のバスキーにより暗号化された暗号化処理済鍵束データの復号化に利用されるものである。鍵束データ復号化処理部２０３ｂは、第１のバスキーにより暗号化された暗号化処理済鍵束データに対して、第２のバスキーにより復号化処理を施し、元の鍵束データと同一の復号化処理済鍵束データを提供するものである。

【００３９】以上説明した鍵束データの送信処理その１によれば、デコーダ認証処理部１０３からＤＶＤ信号処理部１０８へ送信される第１のバスキーを暗号化することにより、バスライン３００上のデータが解析されることによる第１のバスキーの解読を防止することができる。つまり、第１のバスキーが解読されなければ、この第１のバスキーにより暗号化された鍵束データが解析されるのを防止することができ、結果的に、光ディスクデータの不正コピーが防止できる。

【００４０】次に、鍵束データの送信処理その２について説明する。図３は、鍵束データの送信処理その２を実現するための構成を示す図である。図３に示すように、デコーダ認証処理部１０３には、暗号化用データ生成手段としての第１のバスキー生成部１０３ａ、及び暗号化処理手段としてのバスキー暗号化処理部１０３ｃが設けられている。第１のバスキー生成部１０３ａは、上記説明した相互認証処理によりドライブ装置及びデコーダ装置が相互に認証されことを条件として、第１のバスキーを生成するものである。この第１のバスキーは、鍵束データの暗号化に利用されるものである。バスキー暗号化処理部１０３ｃは、第１のバスキーを暗号化して暗号化された暗号化処理済バスキーをバスライン３００へ出力するものである。

【００４１】ここで、バスキー暗号化処理部１０３ｃにおける暗号化処理について説明する。バスキー暗号化処理部１０３ｃには、乱数生成手段としての疑似雑音発生回路１０３ｄ、及び第１の排他的論理和算出手段としての排他的論理和算出回路１０３ｅが設けられている。疑似雑音発生発生回路１０３ｄは、ｎビットの乱数を発生させるものである。乱数は、固定されたものであってもよいし、時間とともに変化するものであってもよい。排他的論理和算出回路１０３ｅは、第１のバスキーと乱数との排他的論理和を算出するものである。また、この排他的論理和の値が暗号化処理済バスキーとして、バスラ

インターフェース３００を介してＤＶＤ信号処理部１０８へ送信される。

【００４２】ＤＶＤ信号処理部１０８には、暗号化処理手段としての鍵束データ暗号化処理部１０８ａ、及び復号化処理手段としてのバスキー復号化処理部１０８ｃが設けられている。バスキー復号化処理部１０８ｃは、バスライン３００を介して送信される暗号化処理済バスキーに対して復号化処理を施し、第１のバスキーと同一の復号化処理済バスキーを提供するものである。ここで、バスキー復号化処理部１０８ｃにおける復号化処理について説明する。バスキー復号化処理１０８ｃには、乱数入力部１０８ｄ、及び第２の排他的論理和算出手段としての排他的論理和算出回路１０８ｅが設けられている。乱数入力部１０８ｄは、疑似雑音発生発生回路１０３ｄで発生された乱数をバスライン３００を介して受取るものである。排他的論理和算出回路１０８ｅは、バスライン３００を介して送信される暗号化処理済バスキーと乱数入力部１０８ｄで受取られた乱数との排他的論理和を算出するものである。また、この排他的論理和の値が第１のバスキーと同一の復号化処理済バスキーとして提供される。

【００４３】鍵束データ暗号化処理部１０８ａは、ＤＲＡＭ１０９から読出される鍵束データに対してバスキー復号化処理部１０８ｃから提供される第１のバスキーにより暗号化処理を施し、暗号化処理済鍵束データを提供する。具体的に説明すると、鍵束データ暗号化処理部１０８ａは、鍵束データと第１のバスキーとの排他的論理和を算出する。つまり、ここで算出された排他的論理和の値が暗号化処理済鍵束データということになる。鍵束データ暗号化処理部１０８ａから提供される暗号化処理済鍵束データは、バスライン３００を介してデコーダ装置２００側へ送信される。

【００４４】ドライブ認証処理部２０３には、暗号化用データ生成手段としての第２のバスキー生成部２０３ａ、及び復号化処理手段としての鍵束データ復号化処理部２０３ｂが設けられている。第２のバスキー生成部２０３ａは、上記説明した相互認証処理によりドライブ装置及びデコーダ装置が相互に認証されことを条件として、第１のバスキーと同一のデータである第２のバスキーを生成するものである。この第２のバスキーは、第１のバスキーにより暗号化された暗号化処理済鍵束データの復号化に利用されるものである。鍵束データ復号化処理部２０３ｂは、第１のバスキーにより暗号化された暗号化処理済鍵束データに対して、第２のバスキーにより復号化処理を施し、元の鍵束データと同一の復号化処理済鍵束データを提供するものである。

【００４５】以上説明した鍵束データの送信処理その２によれば、デコーダ認証処理部１０３からＤＶＤ信号処理部１０８へ送信される第１のバスキーを暗号化することにより、バスライン３００上のデータ解析による第１のバスキーの解読を防止することができる。つまり、第１のバスキーが解読されなければ、この第１のバスキーにより暗号化された鍵束データが解析されるのを防止することができ、結果的に、光ディスクデータの不正コピーが防止できる。

【００４６】次に、鍵束データの送信処理その３について説明する。図３は、鍵束データの送信処理その３を実現するための構成を示す図である。図３に示すように、デコーダ認証処理部１０３には、暗号化用データ生成手段としての第１のバスキー生成部１０３ａ、及び暗号化処理手段としてのバスキー暗号化処理部１０３ｆが設けられている。第１のバスキー生成部１０３ａは、上記説明した相互認証処理によりドライブ装置及びデコーダ装置が相互に認証されことを条件として、第１のバスキーを生成する。この第１のバスキーは、鍵束データの暗号化に利用されるものである。バスキー暗号化処理部１０３ｆは、第１のバスキーを暗号化して暗号化された暗号化処理済バスキーをバスライン３００へ出力するものである。

【００４７】ここで、バスキー暗号化処理部１０３ｆにおける暗号化処理について説明する。バスキー暗号化処理部１０３ｆには、暗号化用データ生成手段としてのレジスタ１０３ｇ、及び第１の排他的論理和算出手段としての排他的論理和算出回路１０３ｈが設けられている。レジスタ１０３ｇは、ｎビットのデータを出力するものである。また、このレジスタ１０３ｇから出力されるｎビットのデータは、記憶手段としてのメモリ１０２に記憶されたプログラムに基づき生成されるものとする。このとき、プログラムに基づくｎビットのデータ生成は、制御手段としてのドライブ制御部１０１により行われるものとする。排他的論理和算出回路１０３ｈは、第１のバスキーとｎビットのデータとの排他的論理和を算出するものである。また、この排他的論理和の値が暗号化処理済バスキーとして、バスライン３００を介してＤＶＤ信号処理部１０８へ送信される。

【００４８】ＤＶＤ信号処理部１０８には、暗号化処理手段としての鍵束データ暗号化処理部１０８ａ、及び復号化処理手段としてのバスキー復号化処理部１０８ｆが設けられている。バスキー復号化処理部１０８ｆは、バスライン３００を介して送信される暗号化処理済バスキーに対して復号化処理を施し、第１のバスキーと同一の復号化処理済バスキーを提供するものである。ここで、バスキー復号化処理部１０８ｆにおける復号化処理について説明する。バスキー復号化処理１０８ｆには、レジスタ１０８ｇ、及び第２の排他的論理和算出手段としての排他的論理和算出回路１０８ｈが設けられている。レジスタ１０８ｇは、ｎビットのデータを出力するものである。また、このレジスタ１０８ｇから出力されるｎビットのデータは、記憶手段としてのメモリ１０２に記憶されたプログラムに基づき生成されるものとする。この

とき、プログラムに基づくｎビットのデータ生成は、制御手段としてのドライブ制御部１０１により行われるものとする。従って、レジスタ１０３ｇから出力されるデータと、レジスタ１０８ｇから出力されるデータとは同一のデータとなる。

【００４９】排他的論理和算出回路１０８ｈは、バスライン３００を介して送信される暗号化処理済バスキーとレジスタ１０８ｇから出力されるｎビットのデータとの排他的論理和を算出するものである。また、この排他的論理和の値が第１のバスキーと同一の復号化処理済バスキーとして提供される。

【００５０】鍵束データ暗号化処理部１０８ａは、ＤＲＡＭ１０９から読出される鍵束データに対してバスキー復号化処理部１０８ｃから提供される第１のバスキーにより暗号化処理を施し、暗号化処理済鍵束データを提供する。具体的に説明すると、鍵束データ暗号化処理部１０８ａは、鍵束データと第１のバスキーとの排他的論理和を算出する。つまり、ここで算出された排他的論理和の値が暗号化処理済鍵束データということになる。鍵束データ暗号化処理部１０８ａから提供される暗号化処理済鍵束データは、バスライン３００を介してデコーダ装置２００側へ送信される。

【００５１】ドライブ認証処理部２０３には、第２のバスキー生成部２０３ａ、及び鍵束データ復号化処理部２０３ｂが設けられている。第２のバスキー生成部２０３ａは、上記説明した相互認証処理によりドライブ装置及びデコーダ装置が相互に認証されることを条件として、第１のバスキーと同一のデータである第２のバスキーを生成するものである。この第２のバスキーは、第１のバスキーにより暗号化された暗号化処理済鍵束データの復号化に利用されるものである。鍵束データ復号化処理部２０３ｂは、第１のバスキーにより暗号化された暗号化処理済鍵束データに対して、第２のバスキーにより復号化処理を施し、元の鍵束データと同一の復号化処理済鍵束データを提供するものである。

【００５２】以上説明した鍵束データの送信処理その３によれば、デコーダ認証処理部１０３からＤＶＤ信号処理部１０８へ送信される第１のバスキーを暗号化することにより、バスライン３００上のデータ解析による第１のバスキーの解読を防止することができる。つまり、第１のバスキーが解読されなければ、この第１のバスキーにより暗号化された鍵束データが解析されるのを防止することができ、結果的に、光ディスクデータの不正コピーが防止できる。

【００５３】

【発明の効果】この発明によれば、光ディスクデータの不正コピーを防止することが可能な光ディスク再生装置及び光ディスク記録再生装置を提供できる。

【図面の簡単な説明】

【図１】この発明の一実施の形態に係る光ディスク装置（光ディスク再生装置及び光ディスク記録再生装置）の概略構成を示す図である。

【図２】バスキーの送信処理その１を実現するための構成を示す図である。

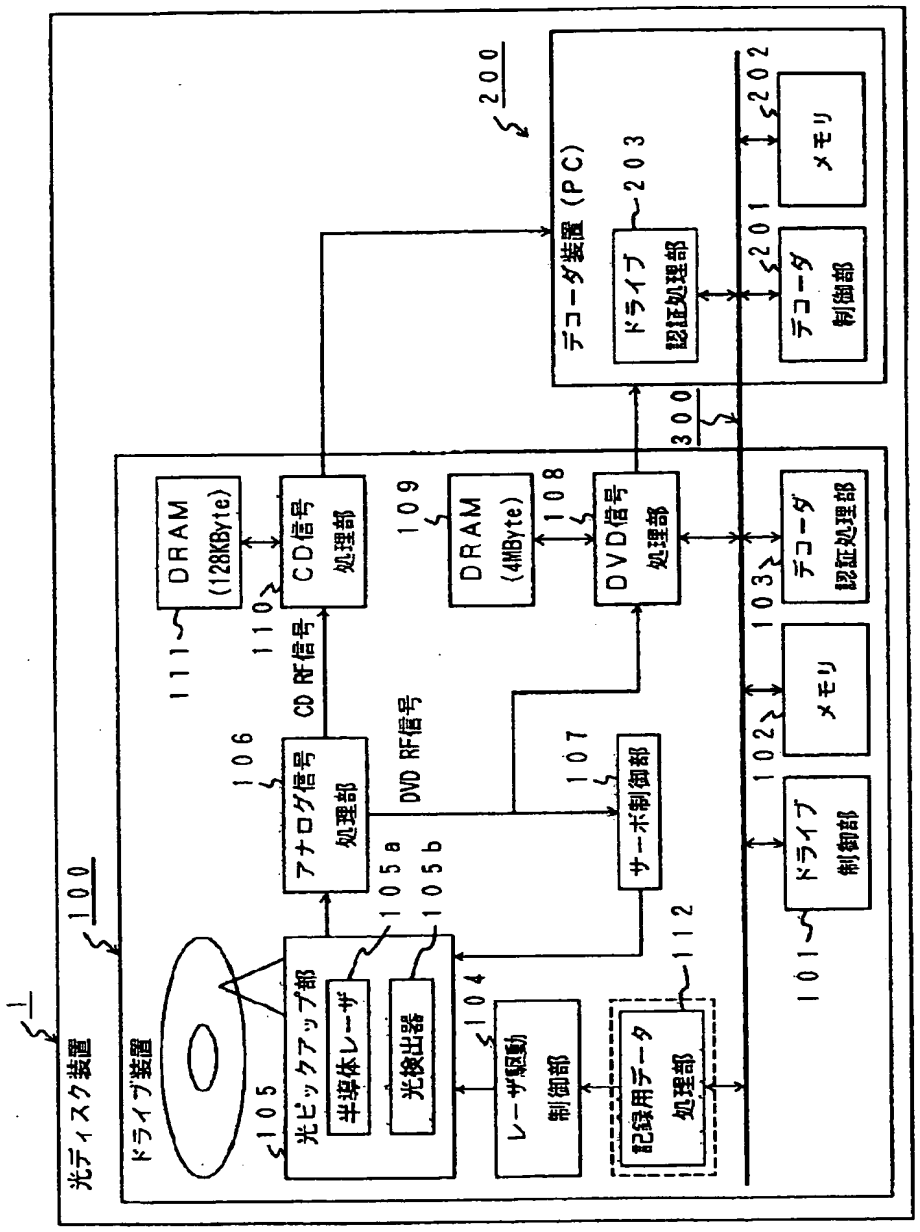
【図３】バスキーの送信処理その２を実現するための構成を示す図である。

【図４】バスキーの送信処理その３を実現するための構成を示す図である。

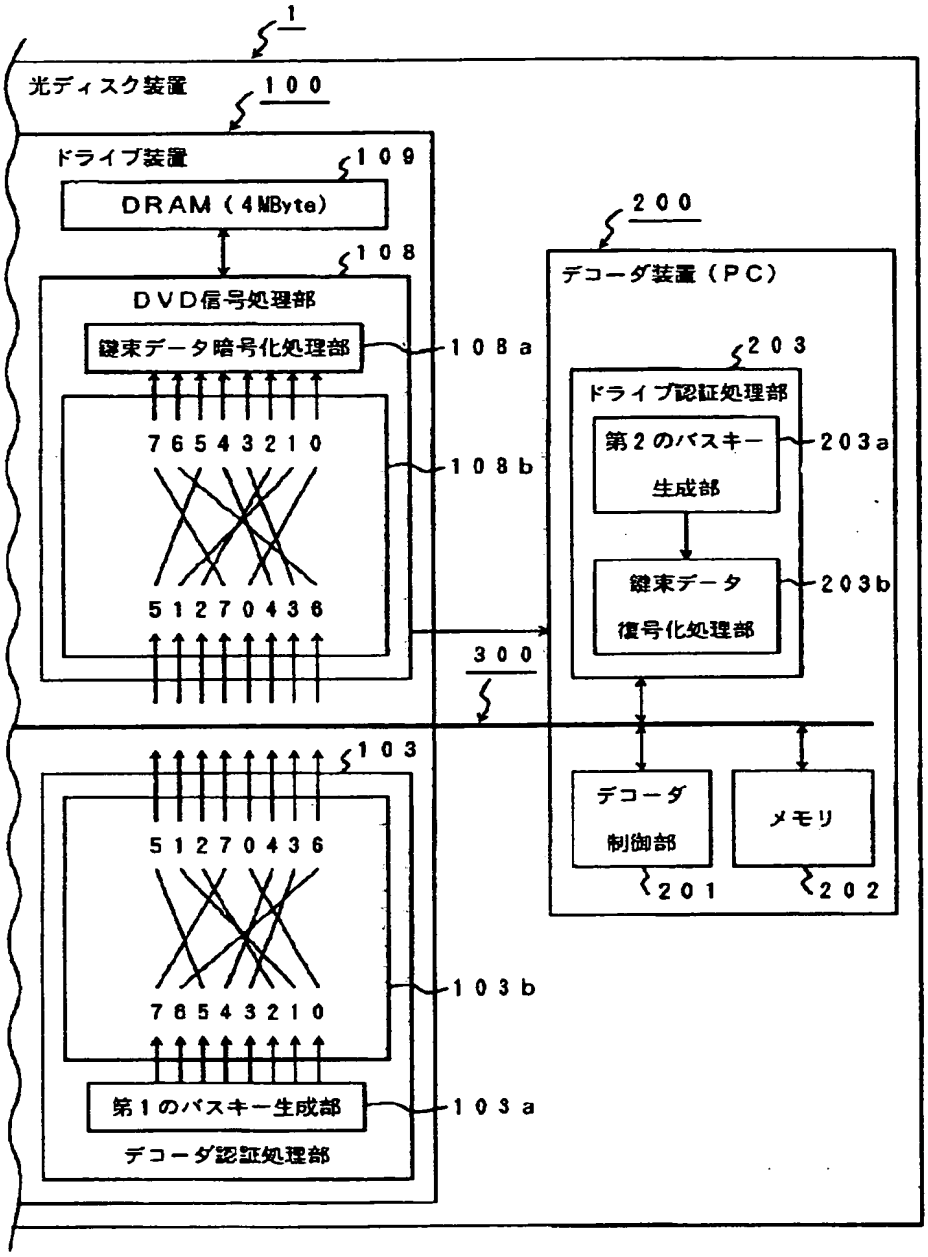
【符号の説明】

１…光ディスク装置
１００…ドライブ装置
１０１…ドライブ制御部
１０２…メモリ
１０３…デコーダ認証処理部
１０８…ＤＶＤ信号処理部
２００…デコーダ装置
２０１…デコーダ制御部
２０２…メモリ
２０３…ドライブ認証処理部
３００…バスライン

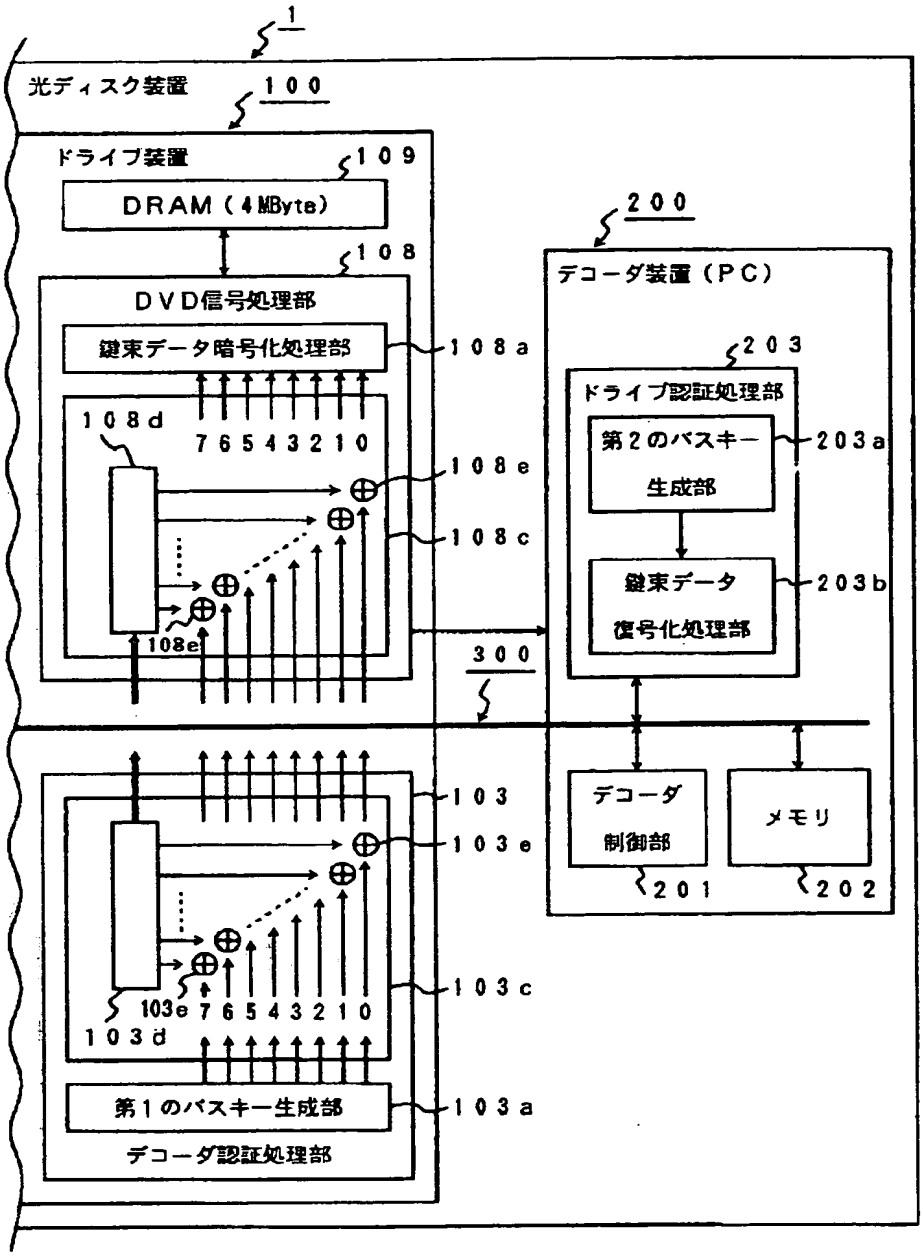
【図1】


1
光ディスク装置
100
ドライブ装置
105
光ピックアップ部
半導体レーザ
光検出器
105a
105b
104
レーザ駆動
制御部
112
記録用データ
処理部
101
ドライブ
制御部
102
メモリ
103
デコーダ
認証処理部
106
アナログ信号
処理部
CD RF信号
DVD RF信号
107
サーボ制御部
111
DRAM
(128KByte)
110
CD信号
処理部
109
DRAM
(4MByte)
108
DVD信号
処理部
300
200
デコーダ装置(PC)
203
ドライブ
認証処理部
201
デコーダ
制御部
202
メモリ

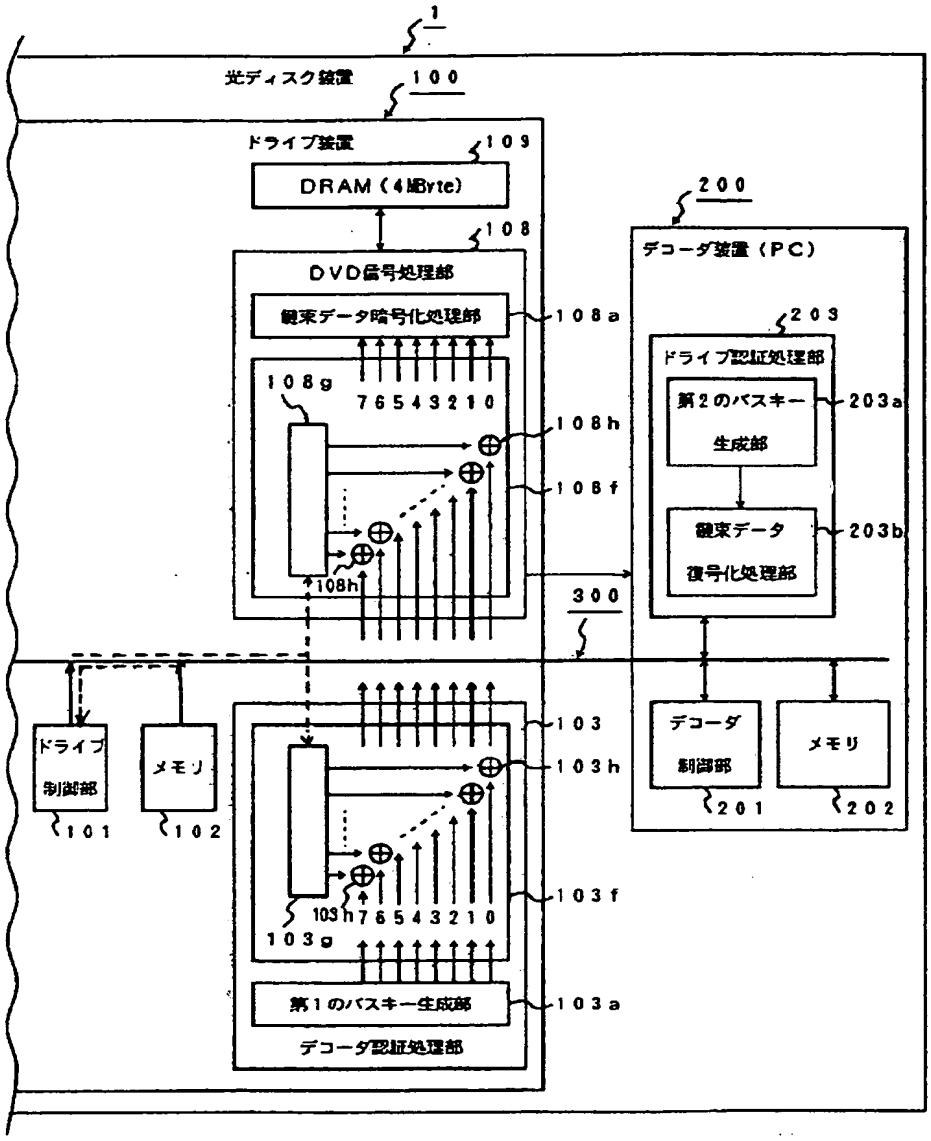
【図2】


1
光ディスク装置
100
ドライブ装置
109
DRAM（4MByte）
108
DVD信号処理部
鍵束データ暗号化処理部
108a
7 6 5 4 3 2 1 0
108b
5 1 2 7 0 4 3 6
300
103
5 1 2 7 0 4 3 6
7 6 5 4 3 2 1 0
103b
第1のバスキー生成部
103a
デコーダ認証処理部
200
デコーダ装置（PC）
203
ドライブ認証処理部
第2のバスキー生成部
203a
鍵束データ復号化処理部
203b
デコーダ制御部
201
メモリ
202

【図３】


1
光ディスク装置
100
ドライブ装置
109
DRAM（4MByte）
108
DVD信号処理部
鍵束データ暗号化処理部
108a
108d
7 6 5 4 3 2 1 0
108e
108c
108e
300
200
デコーダ装置（PC）
203
ドライブ認証処理部
第2のバスキー生成部
203a
鍵束データ復号化処理部
203b
デコーダ制御部
201
メモリ
202
103
103e
103e 7 6 5 4 3 2 1 0
103d
103c
第1のバスキー生成部
103a
デコーダ認証処理部

【図４】



フロントページの続き

(51)Int.Cl.⁶	識別記号	FI	
G11B 20/18	542	G11B 20/18	542Z